Web Results **1 - 10** of about **16,300** for **GPU + encryption + memory + unique key + session key**. (**0.34** secc

Methods and systems for maintaining an encrypted video **memory** ...
Thus, decryptor 312 uses a **unique key** associated with data on surface 304 to ... Notice in this example that the **GPU** comprises **encryption** and decryption ...
www.freepatentsonline.com/20040111627.html - 75k - Cached - Similar pages

Methods and systems for authenticationof components in a graphics ...
A method according to claim 6, wherein the lifetime of the **session key** is the ... that sets a **key** renewal frequency for a layer of video **memory encryption** ...
www.freepatentsonline.com/20030200435.html - 126k - Cached - Similar pages
[More results from www.freepatentsonline.com]

[PPT] Creating Architecture Security Primitives for Secure Software ...
File Format: Microsoft Powerpoint - View as HTML
Shared-**Memory** MP Security Architecture. Nbridge + **GPU**. South Bridge. Secret **Key** ... **Encryption** (AES). Process **unique** ID. Process **Key**. **Session Key** ...
arch.ece.gatech.edu/present/pact04.ppt - Similar pages

[PPT] Longhorn Output Content Protection
File Format: Microsoft Powerpoint - View as HTML
Can't just pass a **key** over the wire; Too expensive to require embedded **unique** keys; Foundation for **Session Key** established using 2048-bit Diffie Hellman ...
download.microsoft.com/download/9/8/f/98f3fe47-dfc3-4e74-92a3-088782200fe7/TWEN05006_WinHEC05.ppt - Similar pages

[DOC] Output Content Protection and Windows Vista
File Format: Microsoft Word - View as HTML
MacroBlock control data is not even the motion vectors, but rather **GPU** ... The **session key** established between the Output **Encryption** APO and the audio codec ...
download.microsoft.com/download/5/D/6/5D6EAF2B-7DDF-476B-93DC-7CF0072878E6/output_protect.doc - Similar pages

[PDF] Chapter 5 REMOTELY KEYED CRYPTOGRAPHICS
File Format: PDF/Adobe Acrobat
asymmetric **encryption** algorithm to either encrypt the secret **key** directly with. the **GPU's** public **key** or to establish a **session key** that is then used to ...
www.springerlink.com/index/p72358g8n4016r37.pdf - Similar pages

[PDF] Chapter 6 RELATED ISSUES
File Format: PDF/Adobe Acrobat
number of frames, the **key** pad can be used to enter a **session key** that the server. and **GPU** will use to establish the keys for **encryption**. If one **key** is used ...
www.springerlink.com/index/t23lj060646g6767.pdf - Similar pages

SN406999554005 - Free60 Wiki
A strong implementation of security would employ, a strong (128-bit+), **unique-key**-per-box cipher, with the **session key** either stored in the CPU silicon, ...
wiki.free60.org/SN406999554005 - 45k - Cached - Similar pages

[PS] Remotely Keyed Cryptographics Secure Remote Display Access Using ...
File Format: Adobe PostScript - View as Text

GPU session key requires that the **key** be exposed only on the smartcard. The proxy ...
When the images are encrypted, the **encryption key** is recorded on ...
www.cs.columbia.edu/techreports/cucs-050-04.ps.gz - Similar pages

[PDF] Remotely Keyed Cryptographics Secure Remote Display Access Using ...
File Format: PDF/Adobe Acrobat - View as HTML
GPU session key requires that the **key** be exposed only on the smartcard. The proxy ...
own **GPU** for **encryption** before sending them to the client. ...
www.cs.columbia.edu/techreports/cucs-050-04.pdf - Similar pages

Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

GPU + encryption + memory + uniq Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

Google Home - Advertising Programs - Business Solutions - About Google

Terms used GPU encryption memory unique key session key Found 52,424 of 201,062

Sort results by relevance
Display results expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: 1 2 3 4 5 6 7 8 9 10 next
Best 200 shown Relevance scale

1 Cryptography as an operating system service: A case study
Angelos D. Keromytis, Jason L. Wright, Theo De Raadt, Matthew Burnside
February 2006 **ACM Transactions on Computer Systems (TOCS)**, Volume 24 Issue 1
Publisher: ACM Press
Full text available: pdf(669.12 KB) Additional Information: full citation, abstract, references, index terms

Cryptographic transformations are a fundamental building block in many security applications and protocols. To improve performance, several vendors market hardware accelerator cards. However, until now no operating system provided a mechanism that allowed both uniform and efficient use of this new type of resource.We present the OpenBSD Cryptographic Framework (OCF), a service virtualization layer implemented inside the operating system kernel, that provides uniform access to accelerator functio ...

Keywords: Encryption, authentication, cryptographic protocols, digital signatures, hash functions

2 GPGPU: general purpose computation on graphics hardware
David Luebke, Mark Harris, Jens Krüger, Tim Purcell, Naga Govindaraju, Ian Buck, Cliff Woolley, Aaron Lefohn
August 2004 **ACM SIGGRAPH 2004 Course Notes SIGGRAPH '04**
Publisher: ACM Press
Full text available: pdf(63.03 MB) Additional Information: full citation, abstract, citings

The graphics processor (GPU) on today's commodity video cards has evolved into an extremely powerful and flexible processor. The latest graphics architectures provide tremendous memory bandwidth and computational horsepower, with fully programmable vertex and pixel processing units that support vector operations up to full IEEE floating point precision. High level languages have emerged for graphics hardware, making this computational power accessible. Architecturally, GPUs are highly parallel s ...

3 Just fast keying: Key agreement in a hostile internet
William Aiello, Steven M. Bellovin, Matt Blaze, Ran Canetti, John Ioannidis, Angelos D. Keromytis, Omer Reingold
May 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 2
Publisher: ACM Press
Full text available: Additional Information: full citation, abstract, references, citings, index

pdf(324.39 KB) terms

We describe Just Fast Keying (JFK), a new key-exchange protocol, primarily designed for use in the IP security architecture. It is simple, efficient, and secure; we sketch a proof of the latter property. JFK also has a number of novel engineering parameters that permit a variety of tradeoffs, most notably the ability to balance the need for perfect forward secrecy against susceptibility to denial-of-service attacks.

Keywords: Cryptography, denial-of-service attacks

4 Architectural Support for High Speed Protection of Memory Integrity and Confidentiality in Multiprocessor Systems

Weidong Shi, Hsien-Hsin S. Lee, Mrinmoy Ghosh, Chenghuai Lu

September 2004 **Proceedings of the 13th International Conference on Parallel Architectures and Compilation Techniques PACT '04**

Publisher: IEEE Computer Society

Full text available: pdf(255.33 KB) Additional Information: full citation, abstract

Recently there is a growing effort in both the architecture and the security community to create a hardware solution for authenticating system memory.As shown in the previous work, hardware-based memory authentication will become a vital component for creating future trusted computing environments and digital rights protection.Almost all these prior work have focused on authenticating memory exclusively owned by a single processing element.However, in today's computing platforms, memory is often ...

5 Cryptography and data security

Dorothy Elizabeth Robling Denning

January 1982 Book

Publisher: Addison-Wesley Longman Publishing Co., Inc.

Full text available: pdf(19.47 MB) Additional Information: full citation, abstract, references, citings, index terms

From the Preface (See Front Matter for full Preface)

Electronic computers have evolved from exiguous experimental enterprises in the 1940s to prolific practical data processing systems in the 1980s. As we have come to rely on these systems to process and store data, we have also come to wonder about their ability to protect valuable data.

Data security is the science and study of methods of protecting data in computer and communication systems from unauthorized disclosure ...

6 A survey on peer-to-peer key management for mobile ad hoc networks

Johann Van Der Merwe, Dawoud Dawoud, Stephen McDonald

April 2007 **ACM Computing Surveys (CSUR)**, Volume 39 Issue 1

Publisher: ACM Press

Full text available: pdf(872.71 KB) Additional Information: full citation, abstract, references, index terms

The article reviews the most popular peer-to-peer key management protocols for mobile ad hoc networks (MANETs). The protocols are subdivided into groups based on their design strategy or main characteristic. The article discusses and provides comments on the strategy of each group separately. The discussions give insight into open research problems in the area of pairwise key management.

Keywords: Mobile ad hoc networks, pairwise key management, peer-to-peer key management, security

7 Key management for encrypted broadcast

Avishai Wool
May 2000 **ACM Transactions on Information and System Security (TISSEC)**, Volume 3 Issue 2
Publisher: ACM Press
Full text available: pdf(220.36 KB) Additional Information: full citation, abstract, references, index terms

We consider broadcast applications where the transmissions need to be encrypted, such as direct broadcast digital TV networks or Internet multicast. In these applications the number of encrypted TV programs may be very large, but the secure memory capacity at the set-top terminals (STT) is severely limited due to the need to withstand pirate attacks and hardware tampering. Despite this, we would like to allow the service provider to offer different packages of programs to the users. A user ...

Keywords: conditional access, pay-per-view

8 Papers: Context-agile encryption for high speed communication networks

Lyndon G. Pierson, Edward L. Witzke, Mark O. Bean, Gerry J. Trombley
January 1999 **ACM SIGCOMM Computer Communication Review**, Volume 29 Issue 1
Publisher: ACM Press
Full text available: pdf(1.43 MB) Additional Information: full citation, abstract, references

Different applications have different security requirements for data privacy, data integrity, and authentication. Encryption is one technique that addresses these requirements. Encryption hardware, designed for use in high-speed communications networks, can satisfy a wide variety of security requirements if the hardware implementation is key-agile, key length-agile, mode-agile, and algorithm-agile. Hence, context-agile encryption provides enhanced solutions to the secrecy, interoperability, and ...

9 Key management for encrypted broadcast

Avishai Wool
November 1998 **Proceedings of the 5th ACM conference on Computer and communications security CCS '98**
Publisher: ACM Press
Full text available: pdf(1.18 MB) Additional Information: full citation, references, citings, index terms

10 Public-key cryptography and password protocols

Shai Halevi, Hugo Krawczyk
August 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 3
Publisher: ACM Press
Full text available: pdf(275.84 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We study protocols for strong authentication and key exchange in asymmetric scenarios where the authentication server possesses ~a pair of private and public keys while the client has only a weak human-memorizable password as its authentication key. We present and analyze several simple password authentication protocols in this scenario, and show that the security of these protocols can be formally proven based on standard cryptographic assumptions. Remarkably, our analysis shows optimal re ...

Keywords: dictionary attacks, hand-held certificates, key exchange, passwords, public passwords, public-key protocols

11 Nark: receiver-based multicast non-repudiation and key management

Bob Briscoe, Ian Fairman
November 1999 **Proceedings of the 1st ACM conference on Electronic commerce EC '99**
Publisher: ACM Press
Full text available: pdf(168.86 KB) Additional Information: full citation, references, citings, index terms

Keywords: Internet, audit trail, key management, multicast, non-repudiation, smartcard, watermark

12 Key management and key exchange: Efficient, DoS-resistant, secure key exchange for internet protocols

William Aiello, Steven M. Bellovin, Matt Blaze, John Ioannidis, Omer Reingold, Ran Canetti, Angelos D. Keromytis
November 2002 **Proceedings of the 9th ACM conference on Computer and communications security CCS '02**
Publisher: ACM Press
Full text available: pdf(118.52 KB) Additional Information: full citation, abstract, references, citings, index terms

We describe JFK, a new key exchange protocol, primarily designed for use in the IP Security Architecture. It is simple, efficient, and secure; we sketch a proof of the latter property. JFK also has a number of novel engineering parameters that permit a variety of trade-offs, most notably the ability to balance the need for perfect forward secrecy against susceptibility to denial-of-service attacks.

Keywords: cryptography, denial of service attacks

13 Level set and PDE methods for computer graphics

David Breen, Ron Fedkiw, Ken Museth, Stanley Osher, Guillermo Sapiro, Ross Whitaker
August 2004 **ACM SIGGRAPH 2004 Course Notes SIGGRAPH '04**
Publisher: ACM Press
Full text available: pdf(17.07 MB) Additional Information: full citation, abstract, citings

Level set methods, an important class of partial differential equation (PDE) methods, define dynamic surfaces implicitly as the level set (iso-surface) of a sampled, evolving nD function. The course begins with preparatory material that introduces the concept of using partial differential equations to solve problems in computer graphics, geometric modeling and computer vision. This will include the structure and behavior of several different types of differential equations, e.g. the level set eq ...

14 Improving key predistribution with deployment knowledge in static sensor networks

Donggang Liu, Peng Ning
November 2005 **ACM Transactions on Sensor Networks (TOSN)**, Volume 1 Issue 2
Publisher: ACM Press
Full text available: pdf(639.52 KB) Additional Information: full citation, abstract, references, index terms

Pairwise key establishment is a fundamental security service for sensor networks. However, establishing pairwise keys in sensor networks is a challenging problem,

particularly due to the resource constraints on sensor nodes and the threat of node compromises. This article proposes to use both *predeployment and postdeployment knowledge* to improve pairwise key predistribution in static sensor networks. By exploiting the predeployment knowledge, this article first develops two key predistrib ...

Keywords: Sensor networks, key management, key predistribution

15 A key-chain-based keying scheme for many-to-many secure group communication

Dijiang Huang, Deep Medhi
November 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 4
Publisher: ACM Press
Full text available: pdf(311.81 KB) Additional Information: full citation, abstract, references, index terms

We propose a novel secure group keying scheme using *hash chain* for *many-to-many* secure group communication. This scheme requires a *key predistribution center* to generate multiple hash chains and allocates exactly one hash value from each chain to a group member. A group member can use its allocated hash values (secrets) to generate group and subgroup keys. Key distribution can be offline or online via the key distribution protocol. Once keys are distributed, this scheme enab ...

Keywords: Hash chain, key chain, many-to-many secure group communication, secure group communication

16 Applications and compliance: Virtual monotonic counters and count-limited objects using a TPM without a trusted OS

Luis F. G. Sarmenta, Marten van Dijk, Charles W. O'Donnell, Jonathan Rhodes, Srinivas Devadas
November 2006 **Proceedings of the first ACM workshop on Scalable trusted computing STC '06**
Publisher: ACM Press
Full text available: pdf(447.59 KB) Additional Information: full citation, abstract, references, index terms

A trusted monotonic counter is a valuable primitive that enables a wide variety of highly scalable offline and decentralized applications that would otherwise be prone to replay attacks, including offline payment, e-wallets, virtual trusted storage, and digital rights management (DRM). In this paper, we show how one can implement a very large number of *virtual* monotonic counters on an untrusted machine with a Trusted Platform Module (TPM) or similar device, without relying on a trusted OS ...

Keywords: certified execution, e-wallet memory integrity checking, key delegation, stored-value, trusted storage

17 Mobile Code and Distributed Systems: The performance of public key-enabled kerberos authentication in mobile computing applications

Alan Harbitter, Daniel A. Menascé
November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security CCS '01**
Publisher: ACM Press
Full text available: pdf(419.31 KB) Additional Information: full citation, abstract, references, citings, index terms

Authenticating mobile computing users can require a significant amount of processing and communications resources-particularly when protocols based on public key encryption are

invoked. These resource requirements can result in unacceptable response times for the user. In this paper, we analyze adaptations of the public key-enabled Kerberos network authentication protocol to a mobile platform by measuring the service time of a "skeleton" implementation and constructing a closed queuing network m ...

Keywords: authentication, kerberos, mobile computing, performance modeling, proxy servers, public key cryptography

18 Wireless application drivers for low-power systems: Reducing radio energy consumption of key management protocols for wireless sensor networks

Bo-Cheng Charles Lai, David D. Hwang, Sungha Pete Kim, Ingrid Verbauwhede
August 2004 **Proceedings of the 2004 international symposium on Low power electronics and design ISLPED '04**
Publisher: ACM Press
Full text available: pdf(102.71 KB) Additional Information: full citation, abstract, references, index terms

The security of sensor networks is a challenging area. Key management is one of the crucial parts in constructing the security among sensor nodes. However, key management protocols require a great deal of energy consumption, particularly in the transmission of initial key negotiation messages. In this paper, we examine three previously published sensor network security schemes: SPINS and C&R for master-key-based schemes, and Eschenhaur-Gligor (EG) for distributed-key-based schemes. We then prese ...

Keywords: key management protocol, sensor network

19 A compiler for analyzing cryptographic protocols using noninterference

Antonio Durante, Riccardo Focardi, Roberto Gorrieri
October 2000 **ACM Transactions on Software Engineering and Methodology (TOSEM)**, Volume 9 Issue 4
Publisher: ACM Press
Full text available: pdf(291.90 KB) Additional Information: full citation, abstract, references, citings, index terms

The Security Process Algebra (SPA) is a CCS-like specification languag e where actions belong to two different levels of confidentiality. It has been used to define several noninterference-like security properties whose verification has been automated by the tool CoSeC. In recent years, a method for analyzing security protocols using SPA and CoSeC has been developed. Even if it has been useful in analyzing small security protocols, this method has shown to be error-prone, as it requires the ...

Keywords: automatic verification, cryptographic protocols, noninterference, process algebra, verification tool

20 Cryptographic protocols/ network security: Efficient self-healing group key distribution with revocation capability

Donggang Liu, Peng Ning, Kun Sun
October 2003 **Proceedings of the 10th ACM conference on Computer and communications security CCS '03**
Publisher: ACM Press
Full text available: pdf(237.61 KB) Additional Information: full citation, abstract, references, citings, index terms

This paper presents group key distribution techniques for large and dynamic groups over unreliable channels. The techniques proposed here are based on the self-healing key distribution methods (with revocation capability) recently developed by Staddon et al.

[27]. By introducing a novel personal key distribution technique, this paper reduces (1) the communication overhead of personal key share distribution from $O(t^2 \log q)$ to $O(t \log q)$, (2) the communication overhead of self-healing key ...

Keywords: group key distribution, key management, self-healing

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next